UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,815	10/31/2001	Richard Paul Tarquini	10016862-1	4734

7590 01/31/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 01/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/003,815	TARQUINI ET AL.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22 are pending in this office action.

Claim Rejections

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

3. Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin et al. (U.S. Patent No. 6,578,147) in view of Vaidya (U.S. Patent No. 6,279,113).

Regarding claims 1, 7, 14, and 19, Shanklin et al. discloses a method/node/ computer readable medium for detecting an intrusion at node of a network comprising:

- Reading a first packet received by the node (col. 3, lines 40-42);
- Determining a first signature of the first packet (col. 3, lines 42-49);
- Comparing the first signature with a signature file comprising a first machine-readable logic representative of a first packet signature (col. 3, lines 42-49)
- Reading a second packet generated by the node in response to reception of the first packet (col. 3, lines 40-42);
- Determining a second signature of the second packet (col. 3, lines 42-49); and

- Comparing the second signature with the signature file further comprising a second machine-readable logic representative of second packet signature (col. 3, lines 42-49).

Shanklin et al. does not teach **identifying the first packet as an intrusion if the first signature corresponds with the first machine-readable logic and the second signature corresponds with the second machine-readable logic**.

Vaidya discloses **identifying the first packet as an intrusion if the first signature corresponds with the first machine-readable logic and the second signature corresponds with the second machine-readable logic** (col. 8, lines 15-39).

It would been obvious to one ordinary skilled in the art at the time invention was made, to combine identifying the first packet as an intrusion if both the first and second signature correspond to the first and second machine-readable logic, as taught by Vaidya, with the method/node/computer readable medium of Shanklin et al. It would have been obvious for such modifications because comparing both incoming packets to a node and outgoing packets from the same node lowers the chance of false positives because it takes two checks of the same packet (once before being acted upon and once after the packet has been received) before a packet is marked as intrusive.

Regarding claims 2, 3, 8, and 9, Shanklin et al. as modified by Vaidya discloses further comprising executing a directive associated with the first/second machine readable logic upon determining the first/second signature corresponds with the first/second machine readable logic (see col. 3, lines 55-65 of Shanklin et al.).

Regarding claims 4, 10, and 15, Shanklin et al. as modified by Vaidya discloses wherein executing a directive associated with the second machine-readable logic further comprises discarding the second packet (see col. 3, lines 55-65 and col. 4, line 54-61 of Shanklin et al.).

Regarding claims 5 and 11, the examiner believes it to be inherent that discarding the second packet further comprises discarding the packet at the network layer of the network stack of the node because any processing done at the packet level is done in the network layer of the network stack.

Regarding claim 6, Shanklin et al. as modified by Vaidya discloses wherein reading a second packet generated by the node in response to reception of the first node further comprises reading a second packet generated by a network stack of an operating system of the node (see fig. 1, ref. num 10a of Shanklin et al., the station is a typical computer that has an operating system utilizing the network stack, since the network stack is the only layer that uses packets).

Regarding claims 12 and 18, Shanklin et al. as modified by Vaidya discloses wherein comparing the first signature with a first instruction set comprising a first set of machine readable logic representative of a packet signature further comprises performing a binary pattern comparison with the first signature and the first set of machine readable logic (see col. 3, lines 46-49 of Shanklin et al.).

Regarding claim 13, Shanklin et al. as modified by Vaidya discloses wherein comparing the second signature with the signatures file further comprises performing a binary pattern comparison with the second signature and the second machine readable logic (see col. 3, lines 40-49 of Shanklin et al.).

Regarding claims 16, 17, 20, and 21, Shanklin et al. as modified by Vaidya discloses wherein the response packet is received by the node and the response packet is generated by the node (see col. 7, lines 24-31 of Shanklin et al., each node receives and generates responses to packets).

Regarding claim 22, Shanklin et al. as modified by Vaidya discloses further comprising determining that the first packet is a probe packet upon determining the signature corresponds with the machine-readable logic (see col. 5, lines 30-55 of Shanklin et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

Primary Examiner
AU 2131
1/26/06